Journal of Security Studies

ISSN: 2148-6166
Year: 26 **Volume:** 26 **Issue:** 1 **June** 2024 **p.**38-51 **Article Type:** Research
Received Date: 26.02.2024 **Accepted Date:** 14.06.2024

Analysing The Effects of Cyber Security on National Security From A Realist Perspective: "Stuxnet" Example

Şeref Çetinkaya[*], Sami Terzi[**]

Abstract: In this study, the effects of providing cyber security on national security are examined from a realistic perspective using the example of the Stuxnet virus. It has been stated that the increasing complexity of cyber threats due to technological advances poses serious risks to states' national security. In the study, the critical role of cyber security in protecting national security is emphasized through the Stuxnet attack. The Stuxnet attack is a cyber-attack on the facilities where Iran carried out its nuclear enrichment program in 2010. As a result of this attack, it was revealed that Iran had both interruptions in its nuclear program and a weakness in cyber security. As such, it is underlined that cyber security can affect the international balance of power and the strategic interests of states. From a realist perspective, since ensuring national security requires a resilient defense against cyber threats and vulnerabilities, it has become necessary to consider cyber security as an important parameter in determining national security policies. This study reveals the interdependent relationship between cyber security and national security in this age when cyberspace has become a very important arena for power struggles. Considering these reasons, it has been recommended that states, which realists consider the main actor in the international system, should make investments that will support their cyber security to protect their national security.

Keywords: security, cyber security, national security, stuxnet, realism.

[*] Dr. Öğr. Üyesi, İstanbul Üniversitesi, Türkiyat Araştırmaları Enstitüsü Avrasya Çalışmaları ABD, seref.cetinkaya@istanbul.edu.tr, ORCID: 0000-0002-6446-2322.
[**] Bilişim Uzmanı, İstanbul Emniyet Müdürlüğü, sterzi@protonmail.com,
ORCID: 0009-0004-1316-3324.

Güvenlik Çalışmaları Dergisi

ISSN: 2148-6166
Yıl: 26 Cilt: 26 Sayı: 1 Haziran 2024 s.38-51 Makale Türü: Araştırma
Makalenin Geliş Tarihi: 26.02.2024 Makalenin Kabul Tarihi: 14.06.2024

Siber Güvenliğin Ulusal Güvenlik Üzerindeki Etkilerinin Realist Perspektif Üzerinden İncelenmesi: "Stuxnet" Örneği

Şeref Çetinkaya, Sami Terzi

Öz: Bu çalışmada, siber güvenliğin sağlanmasının ulusal güvenlik üzerindeki etkilerini, realist bakış açısıyla ve Stuxnet virüsü örneği kullanılarak incelenmiştir. Siber tehditlerin, teknolojik ilerlemelere bağlı olarak giderek karmaşık hale gelmesi, devletlerin ulusal güvenliği açısından ciddi riskler barındırdığı ifade edilmiştir. Çalışmada, Stuxnet saldırısı üzerinden, ulusal güvenliğin korunabilmesinde siber güvenliğin kritik rolüne vurgu yapılmıştır. Stuxnet saldırısı, 2010 yılında İran'ın nükleer zenginleştirme programını yürüttüğü tesislere yönelik yapılan bir siber saldırıdır. Bu saldırı sonucunda, İran'ın hem nükleer programında kesintiler yaşanmış hem de siber güvenlik konusunda zafiyet yaşadığı ortaya çıkmıştır. Bu haliyle siber güvenliğin, uluslararası güç dengesini ve devletlerin stratejik çıkarlarını etkileyebileceğinin altı çizilmiştir. Realist bir bakış açısıyla; ulusal güvenliğin sağlanması, siber tehditlere ve zafiyetlere karşı dirençli bir savunma gerektirdiğinden, siber güvenlik konusunun ulusal güvenlik ile ilgili politikaların belirlenmesi sürecinde önemli bir parametre olarak ele alınması bir zorunluluk haline gelmiştir. Bu çalışmada, siber alanın güç mücadeleleri açısından çok önemli bir arena haline geldiği bu çağda, siber güvenlik ve ulusal güvenlik arasındaki karşılıklı bağımlılık ilişkisi ortaya konmuştur. Bu nedenler ışığında; realistlerin uluslararası sistemde ana aktör olarak ele aldıkları devletlerin, ulusal güvenliklerini korumak amacıyla, siber güvenliklerini sağlamalarına destek olacak yatırımları yapmaları gerektiği tavsiye edilmiştir.

Anahtar Kelimeler: güvenlik, siber güvenlik, ulusal güvenlik, stuxnet, realizm.

Introduction

In the 21st century, scientific and technological developments have led to a rapid digital transformation. The concept of cyber, encountered in this period, has become one of the important and studied concepts of today. Especially with the increasing integration of the internet into daily life at various levels, awareness regarding the cyber domain has grown, leading to the emergence of security issues in this field. The internet, which spans a wide range of areas from personal use at home to use in the infrastructure of very complex facilities, is one of the most important actors in the emergence of the concept of cyber security. Attacks ranging from unauthorized access to bank accounts using the internet to interventions against states' critical infrastructures can occur at different scales and in a very short time. These attacks have reached levels that threaten security both at the individual and state levels (Öğün and Kaya, 2013, p. 145). Considering that there are approximately 5.38 billion internet users worldwide, and this figure corresponds to about 67.9% of the world population (Internet World Stats, 2022), the importance of the cyber domain and its security becomes more evident.

Advancements in the cyber domain bring along serious cyber threats. Increasingly complicated cyber attacks have become a direct threat to national security. In order to make this claim more concrete, this study analyses the cyber-attack carried out by the software/virus/worm named Stuxnet, whose existence was revealed in 2010 and targeted Iran's nuclear facilities, and tries to analyse how a country's national security is affected by this software.

The Stuxnet attack has been a frequently discussed topic since its emergence. This attack, which is still unclear by whom, is evaluated by both cyber security experts and state administrators. This study will examine the importance and impact of ensuring cyber security on national security from a realist perspective.

The study first presents a comprehensive conceptual framework. Then, by analyzing the Stuxnet attack, it is attempted to explain how cybersecurity can play a vital role in national security. In addition, the effects of the Stuxnet attack are discussed from a realist perspective. Emphasis has been placed on how cyber attacks can quickly change the distribution of power in international networks due to their different characteristics and targeted critical infrastructures. In this study, it is also mentioned that cyber security measures have become an important parameter during the formation of national security policies and the importance of countering cyber threats in issues such as ensuring national security, power struggle and protection of interests.

In this study, literature review, case study and data analysis methods were used. A literature review was made through academic publications on national security, cyber security and realism theory, and the Stuxnet attack was taken as a case study. The data obtained from the Stuxnet attack was used to make the link between national security and cyber security concrete and meaningful.

The main purpose of this study is to determine how important the issue of cyber security is in terms of ensuring national security and contributing to the construction of a strong international community in order to combat cyber attacks that may arise in the future. Since ensuring cyber security may lead to a change in the balance of power and strategic interests in the international system, it is recommended that governments, which are the main actors of the realist theory, invest in cyberspace.

Cyber Security and National Security: Definitions and Scope

The concept of security appears as a concept that harbours ambiguity in its definition. Among the most important reasons for this situation are the many variables that emerge during the definition of the concept and the fact that these variables may vary over time. For this reason, it is difficult to make a definition of security that is accepted by everyone and that can be valid for every period (Sancak, 2013, p. 124). Another debate on the concept is related to whether the main focus of the analyses is on "individual", "national" or "international" level (Baylis, 2008, p. 73). Moreover, there are also common approaches such as "protection from dangers and threats, and continuing to exist" that come to the fore in many definitions of the concept of security (Özcan, 2011, p. 447). Until the last quarter of the 20th century, the concept of security was analyzed in terms of being safe from threats and dangers primarily in the military dimension. However, Buzan emphasized the inadequacy of this approach and extended the analysis to include economic, social, political, and environmental dimensions in addition to the military dimension (Buzan, 1983, pp. 214-242). Following this brief introduction to the concept of security, this study analyses the concepts of cyber security and national security, which have become prominent in recent years.

The concept of cyber can be expressed as "electronic environment", but it covers a much wider set of elements in terms of content. The data in the environment where these elements are located and processed consists of sub-elements such as software, system, algorithm (Sağıroğlu, 2018, p. 24). The elements that constitute cyberspace can be counted as internet, mobile phones, computers, energy transmission lines, drone systems, electromagnetic systems, satellite and robot systems (Çifci, 2013, p. 5). In this context, maintaining cyber security goes beyond the internet and becomes more complex, including closed systems.

When the issue of cyber security is considered, it is appropriate to make brief definitions about cybercrime and cyber terrorism, which are among the concepts we encounter, in terms of the integrity of the subject. Cybercrime covers illegal acts committed by using computer systems and/or networks, where the systems used or different systems can be selected as targets (Yazıcıoğlu, 2002, p. 460). According to another definition, cybercrime is defined as the use of computer systems or networks for the purpose of committing an illegal act (Turhan, 2006, p. 31). On the other hand, cyber terrorism refers to planned attacks on any kind of data and information in the cyber domain for political reasons. According to a different definition, the concept of cyber terrorism corresponds to the attacks against the people and institutions of the government in the cyber domain for terrorism or political purposes (Çolak, 2011, p. 81).

One of the indispensable components of cyberspace is - as mentioned before - the internet. The widespread use of the internet has made the control of cyberspace very difficult. Reasons such as the insufficient level of controls on the internet and the low cost of internet use have led to the variety and increase of threats in cyberspace (Çakmak and Demir, 2009, p. 38). When the security problems of other closed circuit systems that make up the cyberspace are added to this increase in Internet-based threats, the issue becomes more complex. In short, cyber security, which can be described as the security of cyberspace, has become more complex. It would not be wrong to state that existential issues such as the security and survival of the government cannot be considered independent of cyber security when the point of digitalisation in today's world is taken into consideration. At this point, the process of identifying and eliminating threats to national security in the cyber area gets more important.

The concept of national security, which is directly related to the issue of continuity, can be defined as the protection of the government against all kinds of political, economic and cultural threats to the indivisible integrity of the state with its country and nation (Ateş, 1996, p. 25). In other words, national security, which includes taking the necessary security measures for the government to sustain its life, to perform its functions and to make this process continuous, should be minimally affected by attacks that may come from the cyberspace. Otherwise, national security vulnerability will be inevitable. At this point, it would be fitting to analyse what a virus software called "Stuxnet", which appeared in Iran in 2010, can cause in order to see at what level the failures in the provision of cyber security can affect national security.

Differentiating Battlefield

Wars are generally fought on land, sea and air. In this context, the fact that the United States established the Air Force Space Command and later replaced it with the United States Space Force on December 20, 2019, as a separate branch of service, reveals the extent of the change (USSF, 2020). It is calculated that the total economic cost of the operations and wars waged by the USA within the borders of Afghanistan, Pakistan and Iraq after the 11 September attacks is 8 trillion dollars (Kimball, 2021). When the losses of soldiers, diplomats and other personnel are taken into account, it is more clearly understood how high the cost of conventional wars is. Furthermore, it should not be ignored that there is no standing army in the regions where these wars and operations are fought.

Iran is another country with which the United States has had problems for many years. Although Iran started nuclear energy studies between 1950 and 1979 as part of a programme called "Atoms for Peace" with the support of various countries, especially the United States, the revolution in Iran and subsequent developments caused the end of support for Iran (Malus, 2018). However, even though Western support was stopped, Iran continued its nuclear work and established its own programme. Certainly, this situation is perceived as a threat by both the United States and Israel. In a possible war, it is clear that the cost of a war against a country that, unlike Iraq and Afghanistan, has a strong and regular army, can make a great number of technological developments and, most importantly, can produce weapons, can be very high both in terms of economic and human losses. Although the studies on nuclear technology often bring the US, Israel and Iran into confrontation, countries can work on alternative ways and operations due to the consequences of possible conflicts. Considering the possible surgical strike; the use of a large number of cruise missiles such as BGM-109 Tomahawk with a unit cost of 2 million dollars (La Grone, 2021) or sending a fleet of fully armed aircraft such as Lockheed Martin F-35 Lightning II with a cost of approximately 200 million dollars (Reuters, 2014) at a cost of more than a billion dollars and conducting operations with uncertain results also carries great risks. It is difficult to conceal the source of such surgical strikes and therefore it becomes almost impossible to deny the operation. For this reason, a surgical strike can also mean a declaration of war. In addition, a 2011 report on Iran's Natanz Nuclear Fuel Enrichment Plant indicated that it was located approximately 90 metres underground (Albright et al, 2022). Therefore, given that cruise missiles or bunker-busting missiles may be ineffective in penetrating such deep facilities, which are likely to be protected by steel-alloy reinforced concrete, it is inevitable that different solutions to the threat will be on the agenda. It is precisely at this point that the use of cyberspace comes to the fore in terms of both low cost and accessibility to the target.

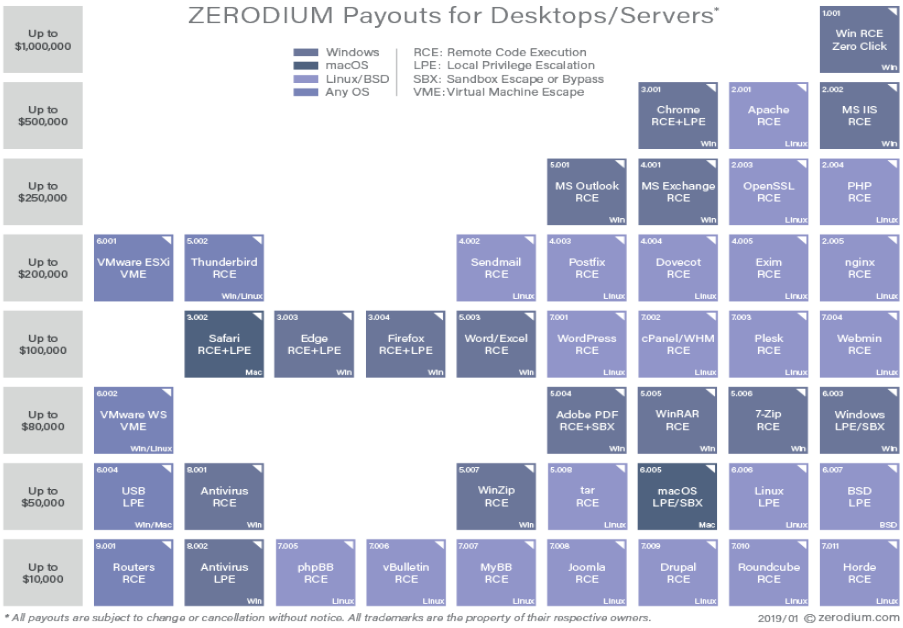
Stuxnet Virus

Sergey Ulasen, a Belarusian antivirus expert, discovered the most complex and unique worm virus ever discovered on 17 June 2010. This worm virus, later known as Stuxnet, was named by combining the words ".stub" and "mrxnet.sys" in its code. This virus was considered as an international cyber-attack element by infiltrating the targeted systems, especially targeting centrifuges in Iranian nuclear facilities (Baezner and Robin, 2017, pp. 4-5).

Stuxnet is recognized as a highly sophisticated piece of software by experts worldwide. There are several reasons for this, but the most important ones are that it was designed for a specific target by performing a comprehensive analysis of the system being attacked, while an expert team can roughly understand the general purpose of an average malicious software within a few minutes, it takes months to understand the target of the Stuxnet virus, and it targets some special industrial equipment that is not accessible to everyone in the market. In the final analysis, it was determined that Stuxnet was designed to decelerate or disrupt centrifuges in Iranian nuclear facilities. It was also found that the virus could infect the target system in different ways. According to this, the virus can infiltrate the target system through various ways such as USB sticks, e-mail attachments, online files and network traffic (Langner, 2011, p. 49). Once the worm virus infects the target system, it scans the system to target specific components and manipulates them. The goal of the Stuxnet attack was to weaken and delay Iran's nuclear programme. Stuxnet used weaknesses in the speed control systems of centrifuges to manipulate their speed. Thus, the normal functioning of the centrifuges was disrupted and they became dysfunctional. With this attack, an important part of the Iranian nuclear programme was neutralised (Falliere et al., 2011, p.3). In addition, Hamid Alipour, deputy head of Iran's Information Technology Company, declared: "Although the main objective of the Stuxnet virus is to destroy industrial systems, its threat to home computer users is serious" (The Sydney Morning Herald, 2010).

As mentioned earlier, Stuxnet was designed using highly sophisticated software engineering. This engineering was specifically designed to analyse the target system, identify the target components and carry out the manipulation (Zetter, 2014, p. 12). Its target is industrial control systems (ICS) and their subset SCADA (Supervisory Control and Data Acquisition), which are used to manage devices in industry (Langner, 2011, p. 50). Even though it has more than 20 times more code than the average malware, almost no bugs have been found. In its current state, the virus greatly shocks cybersecurity and antivirus researchers. Every code to be used in the Stuxnet attack has a task and its planning is close to perfect. The 4 zero-day vulnerabilities in its code are another sophisticated situation. A zero-day vulnerability is the name given to the first day it is discovered that any software can be exploited by exploiting its weakness through manipulation or by making the code non-functional. Since the discovery is new, there is no patch or protection, and this shows how dangerous zero-day vulnerabilities are. In the year 2010, while a total of 12 zero-day vulnerabilities were discovered, Stuxnet alone accounted for 4 (Zerodium, 2016). To understand this unique situation more accurately, it is useful to know that a company called Zerodium pays between $500,000-$1,000,000 (see Figure-1) to those who find and report zero-day vulnerabilities for desktop computers. The same company promises to pay $2,500,000 for mobile zero-day vulnerabilities. In other words, the value of only these 4 zero-day vulnerabilities of Stuxnet has a price between 2 and 4 million dollars (Zerodium, 2023).

Figure-1: The amount of money Zerodium paid for computer vulnerabilities



ZERODIUM Payouts for Desktops/Servers*

Windows
macOS
Linux/BSD
Any OS

RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $1,000,000									1.001 Win RCE Zero Click Win
Up to $500,000							3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win
Up to $250,000						5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux			4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux
Up to $100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux
Up to $80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux

* *All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

2019/01 © zerodium.com

Source: ZERODIUM, "How to Sell Your Zero-Day (0day) Exploit to ZERODIUM", Zerodium, online https://zerodium.com/program.html (access: 21.11.2023).

On the other hand, Stuxnet has root certificates obtained illegally from trusted companies in order to hide itself and install kernel drivers easily. Considering that these certificates are protected in highly secure and internet-free facilities, it should be noted that there is a physical access operation. When all this is considered, it would not be wrong to talk about a cyber weapon designed by a large team spending millions of dollars and taking years to develop. While there are many allegations that the US and Israel are behind the attacks, these have not been officially confirmed. However, it is quite likely that a cyber attack of this level of sophistication was carried out with government power. It is even rare to find a date in Stuxnet when the virus will become invalid. The fact that this was a few days before the change of president after the US elections is considered to be a precaution against the possibility that an attack order approved by the previous US president might not be approved by the next president (Sanger, 2013).

When we look at how the Stuxnet worm works; the Stuxnet worm infects computers via USB drives. The worm first collects information about the operating system and other features of the target computer, then infects the ICS software of the target computer and installs a special virus that affects ICS devices (Moos, 2015, p. 32). This virus disrupts the normal functionality of the SCADA (Supervisory Control and Data Acquisition) software used to control physical components such as rotary axles and other devices, and the same virus generally consists of two different components: an installer and an attacker module. The installer infects computers with Windows operating systems, while the attacker module targets programmable logic controllers (PLCs), which in the case of Stuxnet were Siemens PLCs (Cherry and Langner, 2010). In order to understand the use of this brand of PLCs, it is believed that intelligence was gathered through open-source methods from the images published by Iranian state channels and newspapers to show the nuclear facility to the Iranian people and the world, including images of PLCs and SCADA screens on the computers used to manage these PLCs. The installer spreads via USB sticks, exploiting a vulnerability in Windows related to LNK files. This vulnerability exists in file paths stored in Windows shortcut files. Stuxnet exploited this vulnerability to infect a computer through a shortcut file path in a USB stick. The attacker module is designed to target Siemens PLCs (Al-Rabiaah, 2018). This module consists of two separate components: a kernel module and a user module. The kernel module installs the drivers required for the attack, while the user module installs the code required to manipulate the control systems. This virus, which operates centrifuges in Iranian nuclear facilities at frequencies both faster and slower than normal at intervals, has caused disruptions in nuclear research. It achieves this by inducing the components inside these centrifuges to break apart, forcing them to make contact with each other along with the generated pressures. As a result, there has been a temporary interruption in nuclear studies. During this process, in order to make the SCADA data appear normal, it displayed the normal data it had previously recorded on the operators' computers and disabled the emergency shutdown procedures so that the system could not be shut down when it was understood that there was a mistake in the system (Kaspersky, 2010). With these features, this worm is considered to be the first worm in the world to attack industrial control systems. This worm has caused serious concerns about cyber security by showing the potential impact of cyber attacks. It also demonstrated the ability of governments to use cyber weapons as tools of cyber warfare, which later resulted in many countries establishing cyber warfare budgets and demonstrated a new dimension for warfare. This situation has also led to serious debates in the international community on how to control cyber weapons (Pool, 2013; Hatch, 2018).

Effects of the Stuxnet Virus from a Realism Perspective

Realist theory states that the international system has an anarchic structure and positions the state as the main actor within this structure. States have to ensure their own security in order to maintain their existence in an anarchic structure and for that reason, they determine strategies to protect their interests at the highest level (Stone, 1994, p. 449). In other words, the state will behave in the way that its own interests require. Another prominent concept in realist theory is the concept of power. While it is expressed that the international system is a balance of power, military and political power is emphasised and other elements are ignored. Again, the solution of problems in the international arena will be achieved through the use of force. National security issues occupy the agenda of this theory and, as mentioned before, the way to ensure national security is through the use of force (Votti and Kauppi, 1993; Collins, 2007). To summarise; in the realist theory, ensuring the security of the state is the most important matter and the threats that may arise against this issue can be eliminated through the use of force.

The Stuxnet attack has many effects, especially for Iran. First of all, Iran, which faced the fact that it had difficulty in protecting its nuclear facilities, where it carried out its nuclear work in great secrecy, could not retaliate against this situation. Because the identity of the attackers is unknown (Rosenbaum, 2012). In political terms, Iran has experienced both a credibility problem and a loss of power in the eyes of its own society and the international community. In a sense, the balance of power has been disturbed in an anarchic system. Iran was unable to prevent the cyber-attack on the facility, which it secured militarily, and considered this situation as a serious threat to its national security.

The attack also had effects on the Iranian economy. Especially due to international embargoes causing supply shortages, Iran's loss of centrifuges has constituted a significant cost in this regard. In order to prevent a similar attack, it has become a necessity to take new security measures, which has also caused a separate investment cost. As a result, a new cyber unit was established within the Revolutionary Guards in Iran in November 2011 (Baezner and Robin, 2017, p. 10). Later on, some cyber-attacks against some US companies were associated with Iran's cyber unit, but the accusations could not be fully proven.

The Stuxnet virus was designed directly against the centrifuges at Natanz. The function of the virus was to decrease and increase the speed of the centrifuges to create tension and, with time, to cause the centrifuges to malfunction in such a way that they could not be used (Farwell and Rohozinski, 2011, pp. 24-25). The time between the virus infiltrating the centrifuges and becoming active and causing malfunctioning was almost a year. This shows that Stuxnet was probably a virus "designed to remain hidden for a certain period of time, damage centrifuges and then disappear" (Nakashima and Warrick, 2012). The rapid advancement of technology and the fact that software that can be used for malicious purposes has reached dimensions that can damage the strategic infrastructures of countries has also been an indicator of the diversification of threats to national security. In the face of the diversification of risks and threats, it is a natural consequence that the concept of power also differentiates.

In a sense, the balance of power was restored regardless of the outcome of a military or political action. Another important impact of Stuxnet was in the field of terrorism. The possibility of terrorist groups using such malware to attack countries seems to be very worrying. For this reason, countries that want to protect themselves against threats and survive have to develop a new security paradigm. It has become inevitable for the country, whose security strategies and policies are changing, to invest in different fields in addition to military and political fields.

Conclusion

This cyberattack, executed using the Stuxnet virus, is considered one of the most effective attacks witnessed to date. The attack targeting the facilities in Natanz, where Iran conducts its nuclear enrichment program, rendered thousands of centrifuges unusable and significantly sabotaged the processes related to Iran's nuclear program.

When evaluated from a realist perspective, it becomes possible to observe the contributions of measures taken in the field of cybersecurity to national security. Considering that the digital environment is developing and expanding day by day, it can be stated that managing digital risks and threats is of critical importance in ensuring national security. The Stuxnet incident also revealed weaknesses in the field of cyber security and how a computer virus can pose a great threat to a country. The fact that a country's critical institutions, organisations and infrastructures are exposed to similar cyber-attacks means that its national security may also be at risk. States whose national security is threatened by cyber-attacks and who are helpless against them may not only lose prestige in the international arena in terms of other states and actors, but may also move away from being a deterrent power.

The Stuxnet attack that Iran faced in 2010 also indicates the existence of a potential cyberspace within the international system that could influence the balance of power. Attacks executed by a state with ensuring robust capabilities in the cyber domain, targeting the critical infrastructures of other states, can provide it with strategic and political advantages. This situation underscores that the capacity for cybersecurity has become an exceptionally crucial element in the power struggle within international relations.

The Stuxnet attack and similar cyber threats/incidents demonstrate a close relationship between national security and cybersecurity. Ensuring cybersecurity is crucial for preserving national security and for a state to be strong and deterrent in the international system. Therefore, it is vital to make investments in developing cyber capabilities, stay updated on current scientific and technological advancements, and formulate effective national security strategies to combat cyber threats. Consequently, it is important for states to pursue a dynamic cybersecurity policy and collaborate with relevant parties to protect their interests internationally and mitigate cyber threats.

References

Albright, D., Burkhard, S. ve Hannah, J. (2022). "Iran's Natanz Tunnel Complex: Deeper, Larger than Expected", *Institute For Science and International Security Report*, https://isis-online.org/isis-reports/detail/irans-natanz-tunnel-complex-deeper-larger-than-expected/8

Al-Rabiaah, S. (2018). *The "Stuxnet" Virus of 2010 As an Example of A "APT" and Its "Recent" Variances*, 21st Saudi Computer Society National Computer Conference (NCC).

Ateş, A. (1996). *Milli Güvenlik Siyaseti ve Stratejisi*, İstanbul: Harp Akademileri Basım Evi.

Baezner, M. ve Robin, P. (2017). *Hotspot Analysis: Stuxnet*, Zürich: Center for Security Studies (CSS).

Baylis, J. (2008). Uluslararası İlişkilerde Güvenlik Kavramı, *Uluslararası İlişkiler*, 5(18), 69-85. https://dergipark.org.tr/tr/download/article-file/539876

Buzan, B. (1983). *People, States and Fear: The National Security Problem in International Relations,* Brighton, Harvester Books, Chapel Hill, University of North Carolina Press.

Cherry, S. ve Langner, R. (2010). How Stuxnet Is Rewriting the Cyberterrorism Playbook, *IEEE Spectrum*, https://spectrum.ieee.org/podcast/telecom /security/how-stuxnet-is-rewriting-the- cyberterrorism-playbook

Collins, A. (2007). *Contemporary Security Studies,* New York: Oxford University Press.

Çakmak, H. ve Demir, C. K. (2009). Siber Dünyadaki Tehdit ve Kavramlar, Haydar Çakmak ve Taner Altunok (Ed.), *Suç, Terör ve Savaş Üçgeninde Siber Dünya* içinde (s. 23-55), Ankara: Barış Platin Kitabevi.

Çifçi, H. (2013). *Her Yönüyle Siber Savaş*, İstanbul: TÜBİTAK Popüler Bilim Kitapları.

Çolak, H. (2011). Siber Terör, Yargılama Usulü ve Önleyici Tedbirler, *Kazancı Hakemli Hukuk Dergisi*, S. 79-80, 62-142.

Falliere, N., Murchu, L. O. ve Chien, E. (2011). *W32.Stuxnet Dossier*, Symantec Corporation. Erişinm adresi: https://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf

Farwell, J. P. ve Rohozinski R. (2011). Stuxnet and the Future of Cyber War, *Survival***,** 53, 23-40. doi: 10.1080/00396338.2011.555586

Hatch, B. B. (2018). Defining a Class of Cyber Weapons as WMD: An Examination of the Merits, *Journal of Strategic Security,* 11(1), 43-61. doi: 10.5038/1944-0472.11.1.1657

Internet World Stats. (2023). World Internet Users and Population Stats, https://www.internetworldstats.com/stats.htm

Kaspersky, E. (2010). Stuxnet Worm: Facts and Highlights, Kaspersky Lab. https://www.kaspersky.com/about/press-releases/2010_kaspersky-lab-provides-its-insights-on-stuxnet-worm

Kimball, J. (2021). Costs of the 20-year war on terror: $8 trillion and 900,000 deaths, https://www.brown.edu/news/2021-09-01/costsofwar

LaGrone, S. (2021). Anti-Ship Missiles Top Marines $2.95B Fiscal Year 2022 Wishlist, https://news.usni.org/2021/06/02/anti-ship-missiles-top-marines-2-95b-fiscal-year-2022-wishlist

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon, *IEEE Security & Privacy*, 9(3), 49-51. doi: 10.1109/MSP.2011.67

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare, *Security Studies*, 22, 365-404. doi: 10.1080/09636412.2013.816122

Magnolia Pictures. (2016). Zero Days. United States. Retrieved 2016, https://www.imdb.com/title/tt5446858/. (access: 20.05.2023).

Malus, K. (2018). From "Atoms for Peace" to "JCPOA": History of Iranian Nuclear Development, https://k1project.columbia.edu/content/atoms-peace-jcpoa-history-iranian-nuclear-development

Moos, J. (2015). Cyber Forensics in a Post Stuxnet World, *ITNOW,* 57(4), 32-33. doi:10.1093/itnow/bwv100

Nakashima, E. ve Warrick, J. (2012). Stuxnet was work of U.S. and Israeli experts, officials say, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Pool, P. (2013). War of the Cyber World: The Law of Cyber Warfare, *International Lawyer,* 47(2), 299-323. https://scholar.smu.edu/cgi/viewcontent.cgi?article=1585&context=til

Öğün, M. N. ve Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler, *Güvenlik Stratejileri Dergisi*, 9(18), 145-181. https://dergipark.org.tr/tr/download/article-file/84487

Özcan, A. B. (2011). Uluslararası Güvenlik Sorunları ve ABD›nin Güvenlik Stratejileri, *Selçuk Üniversitesi İİBF Sosyal ve Ekonomik Araştırmalar Dergisi*, 22, 451-470. https://dergipark.org.tr/tr/download/article-file/289003

Reuters. (2014). South Korea To Buy 40 F-35 Jets For $7 Billion, https://www.businessinsider.com/r-south-korea-to-sign-deal-this-month-to-buy-40-f-35-jets-for-7-billion-sources-2014-9

Rosenbaum, R. (2012). .Richard Clarke on Who Was Behind the Stuxnet Attack, http://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/?no-ist

Sağıroğlu, Ş. (2018). Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler, Şeref Sağıroğlu ve Mustafa Alkan (Ed.), *Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık* içinde (s. 21-45), Ankara: BGD Siber Güvenlik ve Savunma Kitap Serisi.

Sancak, K. (2013). Güvenlik Kavramı Etrafındaki Tartışmalar ve Uluslararası Güvenliğin Dönüşümü, *KTÜ Sosyal Bilimler Dergisi*, 3(6), 123-134. https://www.ktu.edu.tr/dosyalar/sbedergisi_69519.pdf

Sanger, D. E. (2013). *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power,* US: Broadway Books.

Stone, A. (1994). What Is a Supranational Constitution? An Essay in International Relations Theory, *The Review of Politics,* 56(3), 441-473. https://openyls.law.yale.edu/bitstream/handle/20.500.13051/5323/What_is_a_Supranational_Constitution_An_Essay_in_International_Relations_Theory.pdf;jsessionid=070CAFDF7AD6443C416D49CE82DFA9FC?sequence=2

The Sydney Morning Herald, Stuxnet mutating, rampaging through Iran, 2010, https://www.smh.com.au/business/stuxnet-mutating-rampaging-through-iran-20100927-15u8o.html

Turhan, O.(2006). Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar), *Planlama Uzmanlığı Tezi*, Ankara: Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği. http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/01/Bilgisayar_Aglari_ile_ilgili_Suclar_OguzTurhan.pdf

USSF (United States Space Force). (2020). United States Space Force history, https://www.spaceforce.mil/About-Us/About-Space-Force/History/

Viotti, P. R. ve Kauppi, M. V. (1993). *International Relations Theory: Realism, Pluralism, Globalism*, New York: Macmillan Publishing.

Yazıcıoğlu, Y. (2002). Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı, *Dokuz Eylül Üniversitesi Uluslararası İnternet Sempozyumu Bildirisi*, İzmir, 451-470.

ZERODIUM, How to Sell Your Zero-Day (0day) Exploit to ZERODIUM, Zerodium, https://zerodium.com/program.html

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon,* US: Broadway Books.